Patch Release Note

Patch 86253-09
For Rapier Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86253-09 for Software Release 2.5.3 on existing models of Rapier series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86253-09.

Base Software Release File	86s-253.rez
Patch Release Date	20-Aug-2004
Compressed Patch File Name	86253-09.paz
Compressed Patch File Size	419420 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.5.3 for Rapier Switches and AR400 and AR700 Series Routers (Document Number C613-10362-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86253-09

Patches 86253-06 and 86253-08 were not released.

Patch 86253-09 includes the following enhancements and resolved issues:

PCR: 03445 Module: IPG

Support has been added for the Ping Polling enhancement. For details, see "*Ping Polling of Device Reachability*" on page 49.

PCR: 03825 Module: IPG Level: 2

The incorrect logical interface was selected for broadcast packets received with a subnet mask that differed from the class mask. This issue has been resolved.

PCR: 03959 Module: PING Level: 3

The ADD PING POLL command did not succeed when executed as part of the boot script if an IPv6 address was specified for the IP parameter. This issue has been resolved.

PCR: 31088 Module: LOG Level: 3

Startup messages were not sent to a syslog server for restarts using the **restart router** command. This issue has been resolved.

PCR: 31225 Module: IPG Level: 3

While the switch was set with a CIDR interface address, when it received an ECHO request with a network broadcast destination address for a class C network, the switch sent the ECHO reply packet. Also, the switch forwarded the ECHO request packet using a broadcast MAC address. These issues have been resolved.

PCR: 40016 Module: FILE Level: 2

A switch reboot could be observed if a filename longer than 23 characters was entered for the **file** parameter of the **show file** and **delete file** commands. This issue has been resolved.

PCR: 40053 Module: PRI Level: 2

A PRI interface was sometimes incorrectly shown as *down* in the output of the **show interface** command when a PPP link was active on the interface. This issue has been resolved.

PCR: 40075 Module: OSPF Level: 2

When the command **set ospf defroute=on** was followed by the command **set ospf defroute=on**, a switch reboot could occur. It could also occur if the command **set ospf defroute=on** was followed by the command **reset ospf**. These issues have been resolved.

PCR: 40116 Module: FIREWALL Level: 3

When the firewall was configured to perform NAT on an interface in conjunction with IP policy filters, Telnet to this interface was not possible. This issue has been resolved.

PCR: 40123 Module: OSPF Level: 2

OSPF did not refresh a network LSA when it received a LSA with errors from another vendor's device. This issue has been resolved.

PCR: 40126 Module: PIM Level: 2

A PIM Dense Mode switch that was not directly connected to the multicast streaming source could incorrectly go into the forwarding state. This issue has been resolved.

PCR: 40177 Module: IPv6 Level: 3

The behaviour of the **set ipv6 nd interface retrans** command was inconsistent. This resulted in the commands **show config dynamic=ipv6** and **show ipv6 ndconfig** not displaying their output. This issue has been resolved.

PCR: 40178 Module: STP Level: 3

When STP was disabled, any changes to the RSTP parameters **maxage, hellotime,** or **forwarddelay** in the **set stp** command were not shown in the **show stp** command. This issue has been resolved.

PCR: 40208 Module: IPV6 Level: 2

IPv6 ND entries were not added to the switch's forwarding database, so IPv6 packets were flooded out all ports. This issue has been resolved.

PCR: 40221 Module: FIREWALL Level: 2

The sequence number and acknowledgement numbers were being updated incorrectly in Microsoft Media Service protocol (MMS) control packets, (which establish and maintain a connection). This issue has been resolved.

PCR: 40226 Module: DHCP Level: 2

If the **create dhcp range** command was used to try and create an invalid IP address range that contained an invalid IP address, then the **delete dhcp range** command was used to delete the invalid IP address, a fatal exception error would result. This issue has been resolved.

PCR: 40244 Module: IPG Level: 2

The switch was unable to correctly filter IGMP messages using the L3 filter. This issue has been resolved.

PCR: 40246 Module: DHCP Level: 2

This PCR obsoletes the change made in PCR 40129. It restores the behaviour of displaying a blank 'ClientID' with status 'inuse' for clients who are using an IP address within the device's DHCP range, but do not have an IP address and client ID mapping in the device's DHCP table. This behaviour allows the detection of PCs in the network that are using static IP addresses without the network administration's permission.

PCR: 40258 Module: SWI Level: 2

MLD Snooping did not read an MLD report as a valid MLD packet when PADN was placed before the Router Alert option. This issue has been resolved.

PCR: 40261 Module: PIM4 Level: 4

PIM counters were not totalling up correctly for erroneous packets if the type of PIM packet was not known. This issue has been resolved.

PCR: 40266 Module: IPSEC Level: 2

Out of sequence IPSEC packets could cause a switch reboot. This issue has been resolved.

PCR: 40268 Module: USER, TTY Level: 3

When the switch was configured with a login account authenticated by the RADIUS server and with RSO also configured, if the switch was accessed through telnet, the switch would accept the telnet session for authentication by RADIUS server if and only if the IP address was allowed by the RSO setting. Multiple user privilege level assignment by RADIUS is now supported as well.

PCR: 40271 Module: IGMP, PIM Level: 2

A static IGMP entry was not created with the **create ip igmp destination** command from a configuration script or after enabling PIM for that interface. A PIM *Join* was also not created. This issue has been resolved. Now a PIM *Join* is sent to the RP following the PIM RP election process.

PCR: 40272 Module: IPG Level: 2

The switch learned an ARP entry for an IP address that was already configured on one of its interfaces. This issue has been resolved, and the receipt of spoofed ARP packets will now generate a log message.

PCR: 40275 Module: IPV6 Level: 3

It was possible to create two identical 6-to-4 tunnels with the same IPv4 destination. This issue has been resolved.

PCR: 40277 Module: IPG Level: 2

BGP routes were not always readvertised to peers after a next-hop route was lost and then reactivated. This issue has been resolved.

PCR: 40279 Module: IPG Level: 2

Occasionally the device suffered a fatal error if it received a large number of directed broadcast packets. This issue has been resolved.

PCR: 40284 Module: PIM Level: 2

When PIM-SM was configured and a very large number of IGMP v2 joins were received, a switch reboot could occur. This issue has been resolved.

PCR: 40285 Module: DHCP Level: 3

Existing options for DHCP policies could not be removed with the **delete dhcp** command. This issue has been resolved.

PCR: 40290 Module: IPG Level: 3

An incorrect nexthop for a RIP route was advertised in RIP messages. This issue has been resolved.

PCR: 40293 Module: FIREWALL Level: 2

Reverse NAT rules for connecting clients from the private-side of the firewall to servers on the public side did not work if the specified REMOTE IP address was in the same subnet as the private interface IP address. This issue has been resolved.

PCR: 40298 Module: TTY Level: 2

When a second device logged in, the CLI command prompt was sometimes not displayed until the user pressed a key. This issue has been resolved so that the prompt is displayed immediately.

PCR: 40299 Module: IPG Level: 2

When the most recently added VLAN was deleted, the switch did not respond correctly to subsequent DHCP *Discover* messages. This issue has been resolved.

PCR: 40305 Module: SWI Level: 2

IGMP *Query* packets sent over a non-master trunk port were incorrectly flooded out the master port of the trunk group. This issue has been resolved.

PCR: 40311 Module: IPG Level: 2

A fatal error sometimes occurred when a large number of IP flows were being deleted when an interface went down. This issue has been resolved.

PCR: 40321 Module: ENCO, IPSEC Level: 2

When EXPIRYKBYTES was set to a low value in an IPSEC policy, it was possible that a memory leak could occur if heavy IPsec traffic was being transmitted while the IPsec SA renegotiation took place. This issue has been resolved.

PCR: 40325 Module: ISAKMP Level: 2

ISAKMP failed to match a remote request to a local IPsec policy if the LADDRESS selector was not specified in the local policy. This prevented the IPSec tunnel from being created. This issue has been resolved.

PCR: 40326 Module: SWI Level: 2

If a multicasting device received multicast packets on a port in one switch instance it could not send them out a port in another switch instance. This issue has been resolved.

PCR: 40346 Module: SSH Level: 3

The **dis ssh user=xx** command incorrectly reported success twice. This issue has been resolved.

PCR: 40349 Module: IPv6 Level: 3

Attempts to ping a site-local address from a global unicast address would fail. This issue has been resolved.

PCR: 40350 Module: OSPF Level: 2

All OSPF packets sent had an IP Precedence of 0 rather than 110. This issue has been resolved.

PCR: 40355 Module: VRRP Level: 2

When an IP interface on which VRRP operated was down, the VRRP should be disabled. If it was enabled, VRRP could transition to "INITIAL" state. This issue has been resolved.

PCR: 40356 Module: BGP Level: 2

1) A switch reboot could be observed if an IP interface was deleted while BGP was learning routes.

2) A switch reboot could be observed if a BGP peer was disconnected while the other peer was learning routes.

3) Excessive log messages were generated when the switch was low on memory.

4) Not all routes were removed from the BGP route table when a peer was disabled.

These issues have all been resolved.

PCR: 40361 Module: SWI Level: 2

When a switch port on which dynamic port security has been enabled was receiving new MAC addresses with at least 20% linerate, dynamic port security entries would not appear in the FDB table for that port. This issue has been resolved.

PCR: 40366 Module: IPG Level: 2

If the switch received fragmented packets at near line speed and Firewall was enabled, a switch reboot could occur. This issue has now been resolved. Also, it was possible that the TCP or UDP ports reported by Firewall 'Ping Of Death' or 'Fragment Attack' events were incorrect. This issue has also been resolved.

PCR: 40385 Module: PPP Level: 3

When an STP of a port belonging to more than one STP was disabled then enabled, only the first STP instance becomes enabled not all instances. This issue has been resolved.

PCR: 40392 Module: TELNET

The new optional parameters **idletimeout** and **maxsessions** have been added to the **set telnet** command. The idletimeout parameter specifies a period of time, in seconds, for the Telnet server's idle timer. The maxsessions parameter specifies the number of concurrent Telnet sessions that are supported by the local Telnet server. The full syntax is:

```
set telnet [termtype=termstring] [insertnull={on|off}]
   [listenport=port] [idletimeout=0..4294967295]
   [maxsessions=0..30]
```

PCR: 40399 Module: IPv6 Level: 3

The **add ipv6 nd** command did not work when the port parameter was specified. This issue has been resolved.

PCR: 40402 Module: IPSEC Level: 2

When two devices (A and B) had an IPsec tunnel connecting them and the default route of device A was to device B, device B had a fatal error. If A lost a link, any packets for that link were delivered to B unencrypted. If these packets were routed through device B to device A, then B recognised the packets as needing to be decrypted and attempted it. This caused a fatal error. This issue has been resolved.

PCR: 40403 Module: BGP Level: 2

Procedures for handling **bgp update** messages which contained an invalid **next_hop** attribute specified in Section 6, RFC1711 were incorrect. This issue has been resolved.

PCR: 40405 Module: ENCO Level: 2

If the ENCO process used to encrypt an ISAKMP packet failed, a switch reboot could occur. This issue has been resolved.

PCR: 40411 Module: IP6 Level: 2

In certain cases where static routes in a multi-path environment were used and routes were changed on the switch, the IPv6 flow table of the switch wasn't refreshed correctly, i.e. an entry in the flow table had no outgoing interface and ND entry. This issue has been resolved.

PCR: 40415 Module: VRRP Level: 2

When a master VRRP router was configured from a boot script, the transition to the MASTER state occurred before the Layer 2 interface had been initialised, preventing the gratuitous ARP from being sent. This issue has been resolved.

PCR: 40417 Module: OSPF Level: 3

When LS Acks (Link State Advert acks) were received, they were compared against the transmitted LSA (Link State Advert). If it was the same, the LSA was removed from the re-transmission list. This issue has been resolved.

PCR: 40419 Module: OSPF, IPG Level: 2

If OSPF was configured using the command **set ospf dyninterface=stub,** to advertise dynamic interfaces such as PPPoE interfaces as stub links, the links were not being advertised as expected. This issue has been resolved.

PCR: 40422 Module: FIREWALL Level: 3

A problem existed when setting non-default Firewall attack trigger levels for SMTP attacks. The **show firewall policy attack** output and dynamically generated configuration scripts were incorrect. This issue has been resolved.

PCR: 40432 Module: SWI Level: 3

There was no support for **enable/disable switch port=x** on trunked ports. This issue has been resolved.

PCR: 40440 Module: CLASSIFIER Level: 2

For those classifiers that specified the IP protocol as a match criterion, the IP protocol number was being stored and displayed in a configuration file as a hexadecimal value rather than a decimal value. This issue has been resolved.

PCR: 40442 Module: IPSEC Level: 2

When an IPSEC policy is used on a PPP link with **iprequest=on**, when the PPP link goes down and IPSEC has traffic to transmit, IPSEC repeatedly attempts to activate the PPP link again. The frequency of the reactivation attempts has been reduced.

PCR: 40446 Module: DHCP Level: 2

In certain situations, if a DHCP client used a DHCP relay agent to request IP addresses from the switch acting as the DHCP server on a different subnet, it was not be able to renew the IP address allocated to it. This issue has been resolved.

PCR: 40451 Module: FIREWALL Level: 2

The "number of hits" counter in firewall's application rules was not incremented correctly. This issue has been resolved.

PCR: 40453 Module: IPG Level: 2

Particular IP packets (unicast destination IP, but multicast destination MAC) could result in a memory leak, which in some cases could cause the

device to stop responding to the command line. This issue has been resolved.

PCR: 40465 Module: PIM6, PIM4 Level: 2

The switch could reboot when a user changed the Rendezvous Point Candidate (RPC) priority in the PIM6 module. This issue has been resolved.

PCR: 40469 Module: SWI Level: 2

IGMP Report packets were not flooded to ports correctly. This issue has been resolved.

PCR: 40470 Module: BGP Level: 2

When BGP redistributed routes, locally imported routes were selected rather than peer learnt routes. This issue has been resolved.

PCR: 40477 Module: TELNET Level: 2

An issue had been introduced in an earlier patch such that the command **telnet <ipaddress>** would fail, giving the error "Error (3033007): Unexpected end of line." This issue has been resolved.

PCR: 40484 Module: SW56 Level: 3

Under certain conditions the Transmit FCS error port counter could increment erroneously. This issue has been resolved.

PCR: 40487 Module: CORE Level: 2

A memory leak could occur when the accessing of the environmental monitoring chip failed. This issue has been resolved.

PCR: 40493 Module: DHCP Level: 3

In certain scenarios when acting as a DHCP server, the switch would send a DHCP ACK to an invalid MAC address. This issue has been resolved.

PCR: 40494 Module: CORE, SWITCH Level: 2

If there was a switch chip lockup, only a log message was recorded, and there was no counter recording the number of switch reboots that occurred. This issue has been resolved.

PCR: 40496 Module: DHCP Level: 2

When DHCP is enabled, it reclaims IP addresses at switch startup to determine if the addresses are in use or not. If, during this process, DHCP was disabled then re-enabled, the switch would not attempt to reclaim the

remaining IP address ranges. This would lead to the rejection of DHCP requests for IP addresses that were still being reclaimed. This issue has been resolved.

PCR: 40506 Module: IGMP Level: 2

When the switch was using Multicast Switch Emulation, then if a snooped IGMP entry for a particular group address had to be removed for one VLAN, even though on other VLANs there were still active clients for that multicast group, some data loss could occur. This issue has been resolved.

PCR: 40510 Module: VRRP Level: 2

A configuration generated with the **create config** or **show config dynamic** commands could under some circumstances, include a **disable vrrp = <vrrpid>** command even if VRRP was enabled. This issue has been resolved.

PCR: 40514 Module: SHOW, CORE Level: 2

The switch would restart after 5 minutes if the switch was in an infinite loop that was calling the hardware watchdog tickle. The restart will now occur after 10 seconds of such looping, and exception 701 will appear in the exception list, with the address of the instruction being executed at that moment, rather than just a log message.

PCR: 40516 Module: DHCP Level: 2

While initialising a range, the switch acting as a DHCP server may release a dynamic entry incorrectly. This issue has been resolved.

PCR: 40528 Module: ASYN Level: 2

Asyn port were locking up after a switch was powered up for more than 24 hours when the **time** had not been set (or if the time was set to an invalid setting). This issue has been resolved.

Features in 86253-08

Patch 86253-06 was not released.

Patch file details are listed in Table 2.

Patch 86253-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

Table 2: Patch file details for Patch 86253-09.

Base Software Release File	86s-253.rez
Patch Release Date	30-Apr-2004
Compressed Patch File Name	86253-08.paz
Compressed Patch File Size	354508 bytes

PCR: 03514 Module: IPSEC Level: 2

An incorrect IPSec Security Association (SA) was used to transmit packets when the SA's IP address was assigned dynamically on another VPN gateway. This issue has been resolved.

PCR: 03924 Module: IPG Level: 2

The CPU can no longer receive multicast traffic when there are no Layer 3 interfaces configured as static multicast senders.

PCR: 03967 Module: IPG Level: 2

RIP did not send the correct next hop address if the route originated from a different subnet to that of the egress interface. This issue has been resolved.

PCR: 03990 Module: OSPF Level: 2

If a route filter was added after OSPF had exported routes to other devices in the same OSPF area, the filtered routes were not purged from the link state database. However, other devices in the same OSPF area did purge the routes from their link state databases. This issue has been resolved.

PCR: 31248 Module: IPG Level: 2

When a packet was destined for a network address, the switch would forward the packet to that network and incorrectly create an ARP request containing the address of the network. This issue has been resolved.

PCR: 40041 Module: FIREWALL Level: 2

If the switch was configured as a redundant load balancer with destination interface rules, and duplicate routs over multihomed interfaces, then there could be intermittent denial of legitimate sessions. This was because the route lookup would return alternating interfaces as the egress interface (e.g. vlan2-1 then vlan2-0). This issue has been resolved.

PCR: 40046 Module: IPG Level: 2

The next hop advertised in a RIP *Response* must be directly reachable on the logical subnet over which the advertisement is made. The device sometimes

advertised the next hop of a route that was not on this subnet. This issue has been resolved.

PCR: 40050 Module: STP Level: 2

Sometimes the switch erroneously transmitted STP BPDUs that contained VLAN tags. This issue has been resolved.

PCR: 40064 Module: SWI Level: 2

The **reset switch** command could cause a switch reboot on Rapier 48 switches. This issue has been resolved.

PCR: 40066 Module: FFS

Users were unaware that the flash file system was initialising on the switch. This issue has been resolved by the adding of a new message which informs users when the FFS initialisation is occurring.

PCR: 40067 Module: MNIX Level: 2

When using PPP multilink, many frames were being incorrectly marked as lost. Depending on the number of PPP links configured, this resulted in degraded performance and an occasional a loss of connectivity. This issue has been resolved.

PCR: 40071 Module: IPG Level: 2

Routing tables were not being updated correctly when better BGP routes were learnt. This issue has been resolved.

PCR: 40080 Module: IPV6 Level: 3

Setting the command **set ipv6 nd** to its default value of 0 was producing an error rather than indicating an unspecified value. This problem has been resolved.

PCR: 40091 Module: IPG Level: 2

When there were multiple routes to the same destination, the wrong port number occasionally appeared in a Layer 3 switch hardware table entry. This could lead to incorrect traffic flow. This issue has been resolved.

PCR: 40095 Module: SWI Level: 3

CPU packets egressed from a mirror port always had a VLAN tag regardless of the egress port tagging. This issue has been resolved.

PCR: 40097 Module: FW Level: 2

Changing the time on the router by using the **set time** command was causing any temporary firewall rules configured, i.e. those rules specified with a TTL parameter, to timeout. This issue has been resolved.

PCR: 40099 Module: VLAN Level:

If a mirror port was configured using the command, **set switch mirror=*port x***, then another port was configured to be *tagged* using the command, **set vlan=*default* port=*y* frame=*tag***, the tagging configured for *port x* would be removed. This issue has been resolved.

PCR: 40100 Module: FIREWALL Level: 2

When a firewall rule was added using the commands,
add firewall policy rule action=nat list=*text file name*
(where the text file contained a list of IP addresses), the device dropped packets that matched the rule parameters in the list, instead of translating them.

This issue has been resolved by ensuring that the device translates the addresses of packets that match the rule parameters and whose addresses exist in the list file, but drops packets whose addresses do not exist in the list file.

For outbound packets that match the rule parameters, but not the list, the rule matching process continues until a matching rule is found. If no matching rule is found, the default rule *allow all* is applied. For inbound packets that match the rule parameters, but not the list, the rule matching process is terminated and the packets will be dropped as they are when **action=allow** is specified.

PCR: 40103 Module: NVS Level:3

The NVS read and write routines were not displaying the correct number for the permanent log entries when the default was changed. This issue has been resolved.

PCR: 40106 Module: FIREWALL Level: 3

The command **add firewall policy dynamic=remote file=*filename.txt*** was not accepted when the filename exceeded eight characters (excluding the three suffix characters). This issue has been resolved by enabling the device to shorten these file names before writing them to the configuration file.

PCR: 40107 Module: SWI Level:3

When a switch port is set with a learn limit, and the packet source address is a broadcast or multicast address. Then, rather than ignoring these addresses the switch was learning them and entering them into its forward database. This issue has been resolved.

PCR: 40112 Module: PIM6 Level: 2

PIM Dense Mode *Graft* and *GraftAck* messages were not being sent. This issue has been resolved.

PCR: 40115 Module: IPv6 Level: 3

The *Fail* counter of the **show ipv6 filter** command was not incrementing beyond one. This issue has been resolved.

PCR: 40119 Module: IPG Level: 2

If a port was added to a VLAN as *tagged* by using the command **set vlan=vlan*x* port=y frame=*tagged***, and then a mirror port was configured, the frames transmitted to the mirror port were correctly transmitted as *untagged*. However, if the configuration was saved and the

switch rebooted, then the mirrored frames contained a VLAN tag. This issue has been resolved to ensure that the mirrored data is always transmitted as *untagged* frames.

PCR: 40121 Module: IPG Level: 3

The **create ip mvr vlan, add ip mvr vlan,** and **destroy ip mvr vlan**, commands were not accepting VLAN IDs greater than 255. This issue has been resolved by enabling these commands to accept VLAN IDs up to 4094.

PCR: 40122 Module: SWI Level: 3

Static MAC addresses could not be added to the hardware MAC tables. This issue has been resolved.

PCR: 40124 Module: IPG, SWI Level: 2

When a tagged port was deleted from a VLAN on a Rapier *i* or AT-8800, all MAC addresses, L3 entries and ARPs learned from the port were removed regardless of VLAN membership. This issue has been resolved by ensuring that only entries learned for the specified VLAN are removed.

PCR: 40129 Module: DHCP Level: 2

When a DHCP client entry was detected as being in use on a VLAN interface, the 'Client ID was not being correctly stored. For example, the Client ID was appearing blank in the **show dhcp client** output. This issue has been resolved.

PCR: 40131 Module: SWMX Level: 2

In rapid STP mode, if a port was disabled, then the command **set stp default** was executed, the port could not be re-enabled. This issue has been resolved.

PCR: 40132 Module: STP Level: 2

In rapid STP mode, the **set stp default** command would not reset the STP default values for Max Age, Hello Time, and Forward Delay. This issue has been resolved.

PCR: 40134 Module: SWI Level:

When a classifier-based hardware filter was added, certain classifier numbers, such as 1023, 1024, 2047, and 2048, would cause the switch to reboot. This issue has been resolved.

PCR: 40137 Module: OSPF Level: 3

OSPF would reject IP packets that, after being reassembled, were larger than the standard buffer size of 1800 bytes. This has been resolved by enabling OSPF to process IP fragments whose reassembled size is up to 64 K bytes long.

PCR: 40138 Module: SWCX Level: 2

The GUI was not recognising an AT-G8SX-01 GBIC. This issue has been resolved.

PCR: 40142 Module: OSPF Level: 2

When an interface that was a designated router (DR) went to the down state, the Network LSA was not being flushed from the routing domain. For compliance with RFC 2328 12.4, the Network LSA will now be flushed out.

PCR: 40143 Module: SWI Level: 2

Previously when 10/100 copper ports were disabled, the link state was automatically taken down. Users are now able to select whether ports are disabled or enabled. The option is applied using the command:

```
disable switch port={port-list|all} [flow=pause]
[link={enable/disable}]
```

When **link** is set to **disable**, the port is electrically disabled (the link is taken down). When the link is set to **enable** the port is disabled, but the link remains up.

PCR: 40147 Module: SWI Level: 2

On an Rapier *i* series switches running STP, if a port was disabled and then re-enabled, the port would not pass any more traffic. This issue has been resolved.

PCR: 40150 Module: PPP Level: 2

When a router uses OSPF over PPP and one of its PPP links was lost, the LS updates were not alerting the router's neighbours (via links on its other interfaces) of the PPP outage. This issue has been resolved.

PCR: 40173 Module: IPv6 Level: 2

The MLDSnoop module was not accepting packets that deviated from the RFCs 2460 and 2711. The issue has been resolved.

PCR: 40174 Module: INSTALL Level: 2

When the command **delete install=preferred** was executed, if file *nvs:gui.ins* did not exist, the command would incorrectly create it. To resolve this issue the command will no longer create this file, and will only write to it if it exists already.

PCR: 40209 Module: SYS Level: 3

The HELP command did not allow extra parameters. This issue has been resolved.

PCR: 40228 Module: VLAN, SW56 Level: 2

PCR 40119 introduced an error that prevented tagged VLANs from operating correctly. Communication between untagged was prevented if one of the ports was also configured as a tagged port. this issue has been resolved.

PCR: 40236 Module: SWI Level: 2

A Layer 3 hardware filter configured to trap packets with the *RouterAlert* option did not always filter MLD packets. This was due to variations in the MLD packet fields. This issue has been resolved

Features in 86253-07

Patch 86253-06 was not released.

Patch 86253-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 03941 Module: FIREWALL Level: 2

TCP *Keepalive* packets for FTP sessions were passing through the firewall during the TCP setup stage with TCP Setup Proxy enabled. *Keepalive* packets include sequence numbers that have already been acknowledged. Such packets now fail stateful inspections and are dropped by the FTP application-level gateway.

PCR: 03961 Module: PIM, PIM6 Level: 2

The PIM-DM prune expiry time was not reset when a *State Refresh* message was received. This issue has been resolved.

PCR: 03997 Module: IPG Level: 3

When policy-based routing was active, IP packets not matching any policy-specific routes were forwarded, even if there was no default policy route. This issue has been resolved. Now, a route whose policy exactly matches the policy of the packet is selected. If an exact match does not exist, a route with the default policy will be used to route the packet. If no route is found, the packet is discarded. The TOS field in incoming IP packets is ignored, so packets with the TOS value set are forwarded using a route with the default policy.

PCR: 31080 Module: IPv6 Level: 2

When a ping was sent to the device's link-local address, the device flooded the ICMP *Reply* packet over the VLAN. This issue has been resolved.

PCR: 31104 Module: OSPF Level: 2

Occasionally when a device rebooted its OSPF routes were missing from the route table. This issue has been resolved.

PCR: 31160 Module: IPG Level: 2

A memory leak occurred if DNS relay was configured, and the device kept receiving DNS *Query* packets. This issue has been resolved.

PCR: 31176 Module: PIM6 Level: 2

PIM6 could not send unicast bootstrap messages to a new neighbour. This issue has been resolved.

PCR: 31178 Module: FIREWALL Level: 4

If the SMTP Proxy detected a third party relay attack, the "`SMTP third party relay attack`" trigger message was not displayed. This issue has been resolved.

PCR: 31200 Module: SWI Level: 2

The forwarding database table sometimes did not update correctly when multiple packets with the same MAC source address were sent to the switch via different ports. This issue has been resolved.

PCR: 31202 Module: QOS Level: 3

The HWQUEUE parameter in the SET QOS HWQUEUE command incorrectly accepted values from 0 to 9999. The upper limit for this parameter is 3. This issue has been resolved. The correct limit is now enforced.

PCR: 31205 Module: VRRP Level: 3

Two VRRP log messages were displayed when they should not have been. The log messages were:

```
Vrrp 1: Vlan vlan2 10 Port Failed decrementing priority by 20
```

```
Vrrp 1: Vlan vlan2 1 Port up incrementing priority by 2
```

This issue has been resolved. These messages are now displayed at the correct time.

PCR: 31220 Module: OSPF Level: 2

OSPF neighbours did not establish the *Full* state when IP route filters were applied. This issue has been resolved.

PCR: 31223 Module: IPV6 Level: 3

The neighbour discovery timeout has been set to 3 seconds in ICMPv6 to speed up Destination Unreachable detection.

PCR: 31224 Module: IPG Level: 3

The *badQuery* and *badRouterMsg* counters in the SHOW IGMP and SHOW IGMPSNOOPING commands were not incrementing correctly. This issue has been resolved.

PCR: 31230 Module: OSPF Level: 3

When an Inter-area route went down and the only other route to the destination was an AS-External route, the AS-External route was not selected. This issue has been resolved.

PCR: 31233 Module: L3F Level: 2

A filter entry was lost when the SET SWITCH L3FILTER ENTRY command did not succeed. This issue has been resolved.

PCR: 31236 Module: IPV6 Level: 3

Link-local addresses can only be unicast addresses. If a link-local address was added as an anycast address, no error message was returned. This issue has been resolved. Now, an error message is returned stating that a link-local address must be a unicast address.

PCR: 31239 Module: IPV6 Level: 3

The Maximum Transmission Unit (MTU) was not always set to the MTU value in the ICMP Packet Too Big Message sent from the device. This issue has been resolved.

PCR: 31247 Module: VLAN, IPG Level: 2

After IGMP snooping was disabled, multicast data was not flooded to VLANs. This was because the multicast route forwarding port map was cleared. This issue has been resolved.

PCR: 31253 Module: SWI, SW56 Level: 2

The forwarding database table sometimes did not update correctly when multiple packets with the same MAC source address were sent to the switch via different ports. This issue has been resolved.

PCR: 31258 Module: IPG, DHCP Level: 2

If DHCP clients do not respond to echo requests, the DHCP server can not detect an addressing conflict, so may offer in-use addresses to clients. This issue has been resolved.

This PCR introduces a new parameter, PROBE, to the CREATE DHCP RANGE and SET DHCP RANGE commands. This parameter allows for address probing using ARP requests and replies instead of the normal ping mechanism. This feature is limited to clients on the same subnet (broadcast domain) as the DHCP server, and therefore can not be used with the GATEWAY parameter.

The new syntax is:

```
CREATE DHCP RANGE=name [PROBE={ARP|ICMP}]
    [other-parameters]

SET DHPC RANGE [PROBE={ARP|ICMP}] [other-parameters]
```

PCR: 31259 Module: DHCP Level: 2

When the DHCP server rejected a *DHCPRequest* message, the requested IP address was not logged correctly. This issue has been resolved.

PCR: 31268 Module: IPG Level: 2

PCR 31128 introduced an issue that occasionally caused a fatal error with IP flows. This issue has been resolved.

PCR: 31270 Module: CURE, IPG, ATK, DVMRP, IPX2, LB, LOG, SNMP, UTILITY Level: 3

Entering "?" after a command at the CLI gives context-sensitive Help about parameters valid for the command. Occasionally, commands (for example, ENABLE IP MULTICASTING) were executed when "?" was entered at the end of the command. This issue has been resolved.

PCR: 40006 Module: LOG Level: 2

Executing the SHOW DEBUG command caused a fatal error if the temporary log had been destroyed with the DESTROY LOG OUTPUT=TEMPORARY command. This issue has been resolved.

PCR: 40007 Module: FIREWALL Level: 2

When an interface-based enhanced NAT was defined in a firewall policy, and a reverse NAT rule was defined to redirect traffic to a proxy server, the reverse NAT did not work correctly. The proxy server did not receive any traffic from the device. This issue has been resolved.

PCR: 40008 Module: NTP Level: 3

When the device operated in NTP Client mode, the SHOW TIME command sometimes displayed the incorrect time. This issue has been resolved.

PCR: 40012 Module: IPG, OSPF Level: 2

The device sometimes rebooted when OSPF on demand was enabled for PPP. This issue has been resolved.

PCR: 40020 Module: SW56 Level: 3

When a port's ingress limit was set to less than 1000 with the INGRESSLIMIT parameter in the SET SWITCH PORT command, sending packets to a tagged port caused FCS errors on transmission. This issue has been resolved.

PCR: 40023 Module: IPG Level: 2

The timeout interval for IGMP group membership now conforms to RFC 2236 for IGMPv2.

PCR: 40038 Module: OSPF Level: 2

After a Summary LSA for the default route in a stub area had been refreshed by an Area Border Router, and the Area Border Router was restarted, the Summary LSA was not advertised into the stub area again. This issue has been resolved.

Features in 86253-05

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86253-05.

Base Software Release File	86s-253.rez
Patch Release Date	26-November-2003
Compressed Patch File Name	86253-05.paz
Compressed Patch File Size	700793 bytes

Patch 86253-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 03781 Module: STP Level: 2

A buffer leak occurred when rapid STP was specified with the SET STP MODE=RAPID command, but STP had not been enabled with the ENABLE STP command. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03873 Module: IPG Level: 4

The STATIC and INTERFACE options have been removed from the PROTOCOL parameter in the ADD IP ROUTE FILTER and SET IP ROUTE FILTER commands. These parameters were redundant because received static and interface routes are always added to the route table.

PCR: 03905 Module: TTY Level: 3

A fatal error occurred in the text editor while selecting blocks and scrolling up. This issue has been resolved.

PCR: 03910 Module: IPG Level: 3

When RIP demand mode was enabled, and one interface changed to a reachable state, the triggered *Request* packet was not sent from that interface, and triggered *Response* packets were not sent from all other RIP interfaces. This resulted in slow convergence of routing tables across the network. This issue has been resolved.

PCR: 03926 Module: PIM Level: 2

Repeated *Assert* messages were sent after the prune limit expired. This issue has been resolved. The default dense mode prune hold time has been changed from 60 seconds to 210 seconds.

PCR: 03940 Module: PKI Level: 1

The following two issues have been resolved:

- Large CRL files were not decoded correctly.
- The certificate database was not validated immediately after the CRL file was updated.

PCR: 03953 Module: SW56 Level: 3

On AT-8800 series switches, strict QoS scheduling is now enforced for ports where egress rate limiting is applied. On Rapier *i* series switches, the same QoS setup is now applied to all of the appropriate ports when setting up egress rate limiting.

PCR: 03970 Module: IPV6 Level: 3

If an IPv6 filter that blocked traffic on a VLAN interface was removed, the traffic was still blocked. This issue has been resolved.

PCR: 03982 Module: FIREWALL Level: 3

The SMTP proxy did not correctly filter sessions where messages were fragmented. This had the potential to prevent the detection of third-party relay attacks. This issue has been resolved.

PCR: 03993 Module: FIREWALL Level: 4

The AUTHENTICATION parameter has been removed from the "?" CLI help for firewall commands. This was not a valid parameter.

PCR: 03996 Module: FIREWALL Level: 2

Occasionally some firewall timers stopped early, resulting in sessions being removed prematurely. Because of this, TCP *Reset* packets could be sent by the firewall before TCP sessions were finished. This issue has been resolved.

PCR: 03997 Module: IPG Level: 3

When policy-based routing was active, IP packets not matching any policy-specific routes were forwarded, even if there was no default policy route. This issue has been resolved. Now, a route whose policy exactly matches the policy of the packet is selected. If an exact match does not exist, a route with the default policy will be used to route the packet. If no route is found, the packet is discarded. The TOS field in incoming IP packets is ignored, so packets with the TOS value set are forwarded using a route with the default policy.

PCR: 31002 Module: UTILITY Level: 2

Sometimes the device rebooted when a severe multicast storm occurred due to a loop in the network. This issue has been resolved.

PCR: 31004 Module: TTY Level: 2

If a SHOW command that displayed a lot of information, such as SHOW DEBUG, was executed when the device's free buffer level was very low, the device sometimes became unresponsive. This could also occur if many SHOW commands were executed through a script. This issue has been resolved.

PCR: 31009 Module: HTTP Level: 3

The server string was not copied correctly into an HTTP file request when loading information from the configuration script. This issue has been resolved.

PCR: 31040 Module: PIM Level: 2

When two devices are BSR candidates, and have the same preference set with the SET PIM BSRCANDIDATE PREFERENCE command, the device with the higher IP address was not elected as the candidate. This issue has been resolved.

PCR: 31041 Module: PIM Level: 3

A *Prune* message sent to an old RP neighbour was ignored when a new unicast route was learned. This issue has been resolved.

PCR: 31042 Module: PIM Level: 3

On Rapier series switches, an *Assert* message was not sent after the prune limit expired. This issue has been resolved.

PCR: 31044 Module: SWI Level: 4

The log message "`IGMP Snooping is active, L3FILT is activated`" has been changed to "`IGMP packet trapping is active, L3FILT is activated`". The revised message is clearer when IGMP is enabled and IGMP snooping is disabled.

PCR: 31052 Module: FIREWALL Level: 3

The following changes have been made to the ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands:

- An IP address range for the IP parameter is now only accepted when enhanced NAT is configured.
- An IP address range for GBLREMOTE parameter is now only accepted when reverse or reverse-enhanced NAT is configured.
- The GBLIP parameter is not accepted for a public interface when enhanced NAT is configured.

PCR: 31058 Module: NTP Level: 3

When the interval between the NTP server and client exceeded 34 years 9 days and 10 hours, the time set on the client was incorrect. This issue has been resolved.

PCR: 31063 Module: IPG Level: 2

MVR was not operating if IGMP had not been enabled. This issue has been resolved.

PCR: 31068 Module: STP Level: 2

A fatal error occurred when the PURGE STP command was executed when STP instances were defined with VLAN members. This issue has been resolved.

PCR: 31071 Module: SWI Level: 4

The warning given when a QoS policy is active on a port operating at reduced speed has been changed to reflect the problem more accurately. The old message was:

```
Warning (2087343): Port <Port num> is currently used in QoS
policy <QoS policy num>, this policy may become incorrect
due to the port bandwidth.
```

The new message is:

```
Warning (2087350): Port <Port num> is operating at less than
its maximum speed: this may affect QoS policy <QoS policy
num>.
```

PCR: 31072 Module: SWI Level: 3

If the DISABLE SWITCH PORT command appeared in the configuration script, an interface could come up even though *ifAdminStatus* was set to 'down'. This issue has been resolved.

PCR: 31082 Module: STP Level: 2

The root bridge did not transmit BPDU messages with changed *hellotime*, *forwarddelay* and *maxage* values. This issue has been resolved.

PCR: 31085 Module: LDAP Level: 3

LDAP could not receive large messages spanning multiple packets. This issue has been resolved.

PCR: 31094 Module: FILE Level: 3

Files with lines over 132 characters in length could not be transferred using TFTP. This limit has now been raised to 1000 characters to match the maximum command line length.

PCR: 31096 Module: FFS Level: 3

The SHOW FILE command caused an error when the displayed file had a duplicate entry due to file size mismatch. This issue has been resolved. An error message is now logged when the SHOW FILE command detects a duplicate file. The first FFS file will be deleted when a duplicate exists.

PCR: 31098 Module: DHCP Level: 3

Static DHCP address ranges were not reclaimed if the *Reclaim* operation was interrupted by the interface going down. This issue has been resolved.

PCR: 31099 Module: FIREWALL Level: 4

In the output of SHOW FIREWALL EVENT command, the DIRECTION of denied multicast packets was shown as "out", not "in". This issue has been resolved.

PCR: 31105 Module: ISAKMP Level: 3

A small amount of memory was consumed by each ISAKMP exchange if an ISAKMP policy's REMOTEID was set as an X.500 distinguished name with the CREATE ISAKMP POLICY command. This issue has been resolved.

PCR: 31106 Module: MLD Level: 2

When the device received a version 1 *Query* packet, it become a non-querier on that interface, even if it should have remained as the querier. This issue has been resolved.

PCR: 31118 Module: SWI Level: 2

When the TYPE parameter was specified for the ADD SWITCH L3FILTER command, the type was sometimes a different value in the device's hardware table. This issue has been resolved.

PCR: 31119 Module: LOG Level: 2

The maximum value that the MESSAGES parameter accepted for the CREATE LOG OUTPUT command was different from the value that could be set with the SET LOG OUTPUT command. The DESTROY LOG OUTPUT command did not release the NVS memory that was reserved for the output. These issues have been resolved.

PCR: 31122 Module: RMON Level: 3

The *etherHistoryIntervalStart* node in the *etherHistoryTable* showed incorrect values for the first and last 30 second interval periods. This issue has been resolved.

PCR: 31127 Module: FIREWALL Level: 2

If a rule based NAT was added to the firewall's public interface, the firewall forwarded ICMP *Request* packets even if ICMP forwarding was disabled. This issue has been resolved.

PCR: 31128 Module: IPG Level: 2

When a large number of directed broadcast packets were received, CPU usage increased up to 100%. This occurred because a log message was generated each time a directed broadcast packet was deleted. This issue has been resolved. Log messages are now rate-limited to a maximum of one log message every 10 seconds for a directed broadcast flow. After the first deletion is logged, subsequent log messages include a counter showing the number of directed broadcast packets in the same flow that were deleted since the last log message.

PCR: 31129 Module: IPX2 Level: 2

A fatal error occurred if IPX was disabled and then re-enabled when there was a high rate of incoming IPX traffic on the device. This issue has been resolved.

PCR: 31132 Module: DHCP Level: 2

The DHCP server did not take any action when it received a DHCP *decline* packet. This was because the device only checked the *ciaddr* field in the packet, and not the *RequestedIPAddress* option. This issue has been resolved.

PCR: 31133 Module: IPG

This PCR introduces an enhancement that extends an issue that was resolved in PCR 03890, in which switch port entries are only created for special router multicast addresses. It is now possible to specify reserved multicast addresses that will be treated as multicast packets from routers. Use the following commands to configure this feature.

ADD IGMPSNOOPING ROUTERADDRESS

Syntax

```
ADD IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]
```

Description

where:

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

This command adds reserved IP multicast addresses to the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SET IGMPSNOOPING ROUTERMODE

Syntax

```
SET IGMPSNOOPING ROUTERMODE=
    {ALL|DEFAULT|IP|MULTICASTROUTER|NONE}
```

Description

This command sets the mode of operation for IGMP Snooping.

If ALL is specified, all reserved multicast addresses (i.e. 2240.0.1 to 224.0.0.255) are treated as router multicast addresses.

If DEFAULT is specified, the following addresses are treated as router multicast addresses:

- IGMP Query: 224.0.0.1
- All routers on this subnet: 224.0.0.2
- DVMRP Routers: 224.0.0.4
- OSPFIGP all routers: 224.0.0.5
- OSPFIGP designated routers: 224.0.0.6
- RIP2 routers: 224.0.0.9
- All PIM routers: 224.0.0.13
- All CBT routers: 224.0.0.15

If IP is specified, addresses that are treated as router multicast addresses are specified with the ADD/DELETE IGMPSNOOPING ROUTERADDRESS command. In this mode, the switch will retain previous addresses that have already been specified.

If MULTICAST is specified, the following addresses are treated as router multicast addresses:

- DVMRP Routers: 224.0.0.4
- All PIM routers: 224.0.0.13

If NONE is specified, no router ports are created.

DELETE IGMPSNOOPING ROUTERADDRESS

Syntax `DELETE IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]`

where

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

Description This command deletes reserved IP multicast addresses from the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SHOW IGMPSNOOPING ROUTERADDRESS

Syntax `SHOW IGMPSNOOPING ROUTERADDRESS`

Description This command displays information about the list of configured IP multicast router addresses currently configured on the switch (Figure 1).

Figure 1: Example output for SHOW IGMPSNOOPING ROUTERADDRESS

```
IGMP Snooping Router Address
-------------------------------------------------------------------------------
IGMP Snooping Router Mode ..... IP

Router Address List
--------------------------------
224.0.0.4
224.0.0.6
224.0.0.80
224.0.0.43
224.0.0.23
224.0.0.15
224.0.0.60
-------------------------------------------------------------------------------
```

PCR: 31134 Module: RSTP Level: 2

Bridges transmitted BPDUs at the rate specified by the local *helloTime* value when they were not the root bridge. This is the behaviour specified in 802.1w-2001. This behaviour can cause instability in the spanning tree when bridges are configured with different *helloTime* values, especially when the root bridge's *helloTime* is significantly less than other bridges in the tree. This issue has been resolved. Non-root bridges now adopt the root bridge's *helloTime* value propagated in BPDUs.

PCR: 31135 Module: IPV6 Level: 3

The ADD IPV6 HOST command accepted an invalid IPv6 address. This issue has been resolved.

PCR: 31140 Module: FIREWALL Level: 4

The firewall sent an erroneous IPSPOOF attack message when processing large packets. This issue has been resolved.

PCR: 31145 Module: SWI Level: 3

The port counters were not incremented:

- *ifInDiscards*
- *ifinErrors*
- *ifOutDiscards*
- *ifOutErrors*

This issue has been resolved.

PCR: 31146 Module: SWI Level: 3

The following SNMP MIB objects could not be set:

- *Dot1dStpPriority*
- *Dot1dStpBridgeMaxAge*
- *Dot1dStpBridgeHelloTime*
- *Dot1dStpBridgeForwardDelay*

This issue has been resolved.

PCR: 31147 Module: DHCP Level: 3

DHCP was incorrectly using the directly connected network interface source IP address as the source IP address of packets it generates. This issue has been resolved. DHCP now uses the local IP address as the source address for the packets it generates when a local IP interface address is set. If a local IP interface address is not set, then it uses the IP address of the interface where packets are sent from as the source address.

PCR: 31148 Module: PIM, PIM6 Level: 2

When the device rebooted with PIM or PIM6 enabled, it sometimes did not send a *Hello* packet quickly enough. This issue has been resolved.

PCR: 31152 Module: DHCP Level: 2

When a DHCP client was in the renewing state, and it sent a DHCP *Request*, the device did not add the ARP entry to the ARP table. Instead, the device generated an ARP *Request* in order to transmit the DHCP *Ack*. This caused a broadcast storm in the network when the client kept sending DHCP *Request*s. This issue occurred because the *ciaddr* field, not the *giaddr* field, was checked in the *Request* packet when the device determined whether to add the ARP entry. This issue has been resolved.

PCR: 31154 Module: STP Level: 4

The current implementation of RSTP conforms to the IEEE standard 802.1w-2001. However, several minor deviations from the standard are possible without having a functional impact on the behaviour of RSTP. These changes are useful for debugging RSTP, and tidy up aspects of RSTP that sometimes have no purpose. The following three variations have been implemented:

- The *Learning* and *Forwarding* flags are set in BPDUs to indicate the state of the Port State Transition state machine.
- The *Agreement* flag is set in BPDUs only when a Root Port is explicitly agreeing to a proposal from a designated port. Do not set the *Agreement* flag in BPDUs transmitted by Designated Ports.
- The *Proposal* flag is not set in a BPDU sent by a designated port once the port has reached the forwarding state.

PCR: 31159 Module: FW, VLAN Level: 2

Static ARP entries sometimes prevented the firewall from working correctly. This is because when an VLAN interface is added to the firewall, the CPU takes over the routing from the switch silicon in order to inspect the packet. Hence all the Layer 3 route entries must be deleted. However, static ARP Layer 3 entries were not being deleted from the silicon. This issue has been resolved. When interface is added to the firewall, all hardware layer 3 routing is now turned off to allow the firewall to inspect packets.

PCR: 31162 Module: SWI Level: 2

A STP topology change incorrectly deleted static ARP entries. This issue has been resolved.

PCR: 31167 Module: IPG Level: 2

IP MVR member ports were not timing out. MVR member ports now timeout in the same way as IP IGMP ports. The timeout values are configured by IGMP. Also, IGMP interfaces were incorrectly being enabled and disabled by MVR. This issue has been resolved.

PCR: 31174 Module: IPG Level: 2

If a device had IPSec and firewall enabled, it could not handle long ICMP packets even when enhanced fragment handling was enabled on the firewall. If a long packet is passed to the firewall for processing, the firewall chains the fragmented packets. The firewall can process chained packets, but IPSec could not process these packets, and dropped them. This was only an issue for packets between 1723 and 1799 bytes long. This issue has been resolved. The way IP processes fragmented packets has been changed so that IPsec no longer drops chained packets.

PCR: 31177 Module: SWI Level: 2

On a Rapier 48, after an IP interface was added to a protected VLAN, the switch's MAC address was registered as static in the switch forwarding database, and had an incorrect port number. This information was shown in the output of the SHOW SWITCH FDB command. This issue has been resolved.

PCR: 31180 Module: USER Level: 2

The following commands did not require security officer privilege when the device was in security mode, but this privilege should have been required:

- ADD USER
- SET USER
- DELETE USER
- PURGE USER
- ENABLE USER
- DISABLE USER
- RESET USER

This issue has been resolved. Security officer privilege is now required for these commands when security mode is enabled with the ENABLE SYSTEM SECURITY_MODE command.

PCR: 31190 Module: SWI, SW56 Level: 2

When static port security was enabled with the RELEARN parameter in the SET SWITCH PORT command, and a switch port was reset or unplugged, the MAC entries were removed (unlearned) from the forwarding database table. The MAC entries should only be removed when dynamic port security is in use. This issue has been resolved.

PCR: 31194 Module: BGP, IP Level: 3

When executing the command:

```
ADD IP ROUTEMAP ENTRY SET ASPATH
```

followed by the command:

```
ADD IP ROUTEMAP ENTRY COMMUNITY ADD=YES
```

where the values for ROUTEMAP and ENTRY were the same in both commands, the second command failed and returned a "`ROUTEMAP clause already exists`" error message. This issue has been resolved.

Features in 86253-04

Patch file details are listed in Table 4:

Table 4: Patch file details for Patch 86253-04.

Base Software Release File	86s-253.rez
Patch Release Date	17-October-2003
Compressed Patch File Name	86253-03.paz
Compressed Patch File Size	585295 bytes

Patch 86253-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 02414 Module: IPV6, SWI, IPG, VLAN

MLD snooping is now supported on AT-9800 Series Switches and Rapier *i* Series Switches. For details, see "*MLD Snooping*" on page 45.

PCR: 02577 Module: IPG, LOG Level: 4

The ability to log MAC addresses whenever the ARP cache changes has been added. To enable this, use the command:

```
ENABLE IP ARP LOG
```

To disable it, use the command:

```
DISABLE IP ARP LOG
```

The logging of MAC addresses is disabled by default. Use the SHOW LOG command to view the MAC addresses that have been logged when the ARP cache changes.

PCR: 03162 Module: IPV6 Level: 3

The performance of IPv6 has been improved by introducing IPv6 flows.

PCR: 03268 Module: SWI Level: 1

When using MVR on a Rapier 48 or Rapier 48*i*, multicast packets were not forwarded correctly between ports 1-24 and 25-48. This issue has been resolved.

PCR: 03409 Module: SWI Level: 2

The switch filter was not operating correctly after a boot cycle. This issue has been resolved.

PCR: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03560 Module: IPV6 Level: 2

A fatal error sometimes occurred when IPv6 multicast packets were forwarded via an interface that went down and then came back up. This issue has been resolved.

PCR: 03598 Module: ETH, IPG, IPv6, IPX, PORT, PPP. Level: 3

After about 250 days, commands such as SHOW BRIDGE COUNT were not displaying the correct number of seconds for *Uptime* and *Last Change At*. days. This issue has been resolved.

PCR: 03616 Module: IPG Level: 4

Three new commands have been added to enable and disable transmission of the following ICMP messages: *Network Unreachable*, *Host Unreachable,* and all *Redirect* messages.

The commands are:

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

SHOW IP ICMPREPLY
```

For details, see "*Enable and Disable ICMP Messages*" on page 43.

PCR: 03622 Module: ENCO Level: 2

Interoperating with other vendors implementations of ISAKMP was occasionally causing errors following key exchanges. This relates to differing implementations of the RFC regarding the retention of leading zeros. This issue has been resolved by modifying the software to retain leading zeros. An additional command provides compatibility with routers that still use previous software versions. The command details are:

```
SET ENCO DHPADDING={ON|OFF}
```

This command controls the padding process for Diffie Hellman generated values. This may be required when interoperability is required with other vendor's equipment that uses the Diffie Hellman algorithm.

The DHPADDING parameter specifies whether the Diffie Hellman generated values should be padded or not. If ON is specified, then leading zeros will be inserted into the generated values. If OFF is specified, then the generated values will not be padded. The default is ON.

For example, to turn off the Diffie Hellman padding, use the command:

```
SET ENCO DHPADDING=OFF
```

Also, the output of the SHOW ENCO command now contains a new line showing the setting for DHPADDING.

PCR: 03704 Module: BGP Level: 2

BGP was importing the best route from IP without checking whether the route was *reachable*. BGP now selects the best *reachable* route. If there are no *reachable* routes, BGP will select the best *unreachable* route.

PCR: 03710 Module: PIM, PIM6 Level: 2

The list of multicast groups for each Rendezvous Point occasionally became corrupted, and this could cause a fatal error. This issue has been resolved.

PCR: 03723 Module: BGP Level: 2

BGP routes that were added after a summary aggregate route had been formed were not suppressed. This issue has been resolved: all routes added after summary aggregate route creation are also now suppressed.

The SHOW BGP ROUTE command displayed unselected routes as the "best" route, until they had been processed. This issue has been resolved.

When a single route was deleted from an aggregate route, the aggregate route was deleted, even if it contained other routes. This issue has been resolved.

PCR: 03726 Module: TTY, USER Level: 3

The time recorded when a user logged in was overwritten when the same user logged in a second time while the original connection was still active. This meant the SHOW USER command displayed the same time for both connections. This issue has been resolved.

PCR: 03733 Module: IPV6 Level: 3

When an oversize packet (PMTU) was received, an error message was not returned, even when IPv6 flow was enabled. This issue has been resolved.

PCR: 03734 Module: IPG Level: 2

With static multicasting enabled on two VLANs, only the first few multicast packets of a stream were L3 forwarded. This issue has been resolved.

PCR: 03751 Module: MLDS Level: 3

The MLD snooping entries registered on a port were not removed when the port went down or was unplugged. This issue has been resolved.

PCR: 03757 Module: BGP Level: 2

Route flapping occurred with BGP when an interface went down. This issue has been resolved.

PCR: 03771 Module: SWI Level: 2

When ingress rate limiting was used on Rapier switch ports, TCP sessions sometimes obtained a throughput that was lower than the configured ingress rate limit. This issue has been resolved.

PCR: 03780 Module: INSTALL Level: 3

If a configuration file had a long file name, the SHOW CONFIG command displayed the file name using the shortened DOS 8.3 format (where file names are 8 characters long, with extensions of 3 characters). This issue has been resolved so that long configuration file names are now displayed using the DOS 16.3 format (where file names are up to 16 characters long).

PCR: 03789 Module: ETH Level: 2

When a 4-port ETH PIC card was installed, the output of the SHOW IP INTERFACE command showed the ETH port as Down, but the link LEDs on the card were lit. This issue has been resolved. The SHOW command now shows the correct link status. The link will go down after 90 seconds if no inbound traffic is received. When inbound traffic is received the link will come up.

PCR: 03790 Module: SWI Level: 2

When a tagged port was deleted from a VLAN that was in the default STP, and the port was then added to the VLAN again, communications were sometimes not resumed on that port. This issue has been resolved.

PCR: 03798 Module: IKMP Level: 3

ISAKMP did not support the IPSec message option *ID_IPV6_ADDR_SUBNET* (RFC 2407, 4.6.2.7). ISAKMP was using the *ID_IPV6_ADDR* (RFC 2407, 4.6.2.6) option instead. This issue has been resolved.

PCR: 03801 Module: MLDS Level: 2

MLD and MLD Snooping accepted MLD *Query* packets with a hop limit greater than 1. Duplicate packets were forwarded when the hop limit was not 1 and the payload was 0::0. This issue has been resolved. MLD and MLD Snooping now require the hop limit to be 1.

PCR: 03806 Module: VRRP Level: 4

After the SHOW VRRP command was executed, incorrect trigger messages were entered into the log. This issue has been resolved.

PCR: 03809 Module: SWI Level: 2

An additional check has been added for unknown GBIC models to determine if they are copper or fibre.

PCR: 03817 Module: IPV6 Level: 2

A fatal error occurred when IPv6 fragmented a packet. Also, when a large fragmented ICMP echo request packet was received, the reply may not have been fragmented and so may have exceeded the MTU for the interface it was sent on. These issues have been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03839 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 ping packet length exceeded 1453 bytes. This issue has been resolved.

PCR: 03843 Module: DHCP Level: 2

When some DHCP entries were in *Reclaim* mode, and all interface links related to the range of these entries went down, these DHCP entries were stuck in *Reclaim* mode. This issue has been resolved.

PCR: 03847 Module: TTY Level: 3

Entering Ctrl-N caused some terminals to expect Shift Out ASCII characters. This issue has been resolved.

PCR: 03850 Module: FFS Level: 3

Files were not displayed in the SHOW FFILE command output, after entering "Q" at the CLI to quit from a previous prompt. This issue has been resolved.

PCR: 03852 Module: IPG, IPV6 Level: 2

PIM SM did not establish a BSR candidate between two AR720 routers with PPP over SYN. This issue has been resolved.

PCR: 03854 Module: SWI Level: 2

When INGRESSLIMIT parameter in the SET SWITCH PORT command was set to 64kbps, the switch received packets intermittently rather than continuously. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03868 Module: IPG Level: 3

The *ipForwDatagrams* SNMP MIB object was incremented when it should not have been. This issue has been resolved.

PCR: 03870 Module: SWI, VLAN Level: 3

On Rapier 48*i* switches, mirror port information was repeated in the output of the SHOW VLAN command. This issue has been resolved.

PCR: 03871 Module: FIREWALL Level: 2

The HTTP proxy sometimes allowed URL requests that should have been denied. Also, the HTTP proxy denied all URLs that contained a deniable keyword, even when some URLs with that word had explicitly been allowed. These issues have been resolved.

PCR: 03874 Module: DHCP Level: 3

For parameters that accept a list of IP addresses in a DHCP command (such as LOGSERVER in the ADD DHCP POLICY command), the list is now limited to a maximum of 32 IP addresses.

PCR: 03875 Module: IPG Level: 2

Sometimes OSPF routes were not entered in the IP route table. This issue has been resolved.

PCR: 03876 Module: PING Level: 2

A fatal error occurred if the TRACE command was executed when a trace was already in progress. This issue has been resolved.

PCR: 03878 Module: SWI Level: 2

The layer 3 filter was matching a layer 3 packet incorrectly when the egress port was specified by the filter. This issue has been resolved.

PCR: 03883 Module: IPG Level: 3

Some IP addresses were not displayed correctly in log messages. This issue has been resolved.

PCR: 03884 Module: IPG Level: 2

The IGMP MVR membership timeout was not operating correctly. Membership of a multicast group is now eliminated when it times out. Also, *Leave* messages were not being processed correctly, which sometimes delayed the membership timeout. These issues have been resolved.

PCR: 03888 Module: DHCP, TELNET Level: 2

When the device was configured as a DHCP server, a fatal error sometimes occurred when a telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03890 Module: IGMP, SWI Level: 2

The switch was adding a router port for multicast packets to destinations with an address in the range 224.0.0.x. Switch port entries are now only created for special router multicast addresses.

PCR: 03895 Module: DHCP Level: 2

If the DHCP server had a policy name greater than 5 characters long, and a very long MERITDUMP or ROOTPATH value, the device could not correctly create the configuration. This issue has been resolved.

PCR: 03896 Module: TTY Level: 3

A fatal error occurred when a long string of text was pasted over an existing long string of text at the CLI. This issue has been resolved.

PCR: 03898 Module: ETH Level: 3

An ETH interface was sometimes shown as *Up* in the output of the SHOW INTERFACE command when it was actually *Down*. This issue has been resolved.

PCR: 03902 Module: FIREWALL Level: 3

Under some circumstances traffic did not have NAT applied if a standard subnet NAT rule was added to a public interface. Such rules did not correctly match incoming traffic when the REMOTEIP parameter in the ADD FIREWALL POLICY RULE command was not specified, and the destination IP address was not the interface's actual IP address. If this situation occurred, traffic was redirected back out the public interface. This issue has been resolved.

PCR: 03906 Module: SWITCH Level: 2

Software emulation of layer 3 hardware filtering was not operating correctly. Packets that the switch had no routing information for were filtered incorrectly. The first packet of a flow that should have been dropped was not dropped, and a flow that should have been allowed was being dropped. This issue has been resolved.

PCR: 03907 Module: IPV6 Level: 2

The CREATE CONFIG command did not generate the TYPE parameter for ADD IPV6 INTERFACE commands. This issue has been resolved.

PCR: 03911 Module: SWI Level: 3

The ADD SWITCH FILTER command returned an incorrect error message if a broadcast address was specified for the DESTINATION parameter. This issue has been resolved.

PCR: 03914 Module: IPG, VLAN Level: 3

When IGMP snooping was disabled with the DISABLE IGMPSNOOPING command, IGMP packets were not flooded. This issue has been resolved.

PCR: 03921 Module: IP ARP Level: 3

ARP requests with invalid source MAC and IP addresses were being processed, but should have been dropped. This issue has been resolved.

PCR: 03925 Module: IPV6 Level: 3

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03928 Module: IKMP Level: 2

ISAKMP in *aggressive* mode did not establish a connection when the peer client sent 10 or more payloads. This issue has been resolved.

PCR: 03931 Module: IPSEC Level: 3

The IPSec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03934 Module: IPSEC Level: 2

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03935 Module: ISAKMP Level: 3

ISAKMP debug messages now correctly output IPv6 addresses when using IPv6, and IPv4 addresses when using IPv4.

PCR: 03936 Module: IKMP Level: 3

When ISAKMP was used with IPv6, an incorrect IP address was displayed in the output of the SHOW ISAKMP EXCHANGE command. This issue has been resolved.

PCR: 03938 Module: IKMP Level: 3

DHEXPONENTLENGTH parameter in the CREATE ISAKMP POLICY command was not accepted when creating ISAKMP policies that used IPv6. This issue has been resolved.

PCR: 03939 Module: IPV6 Level: 2

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03946 Module: IPSEC Level: 3

When IPSec was used with IPv6, an incorrect IP address was displayed in the output of the SHOW IPSEC SA command. This issue has been resolved.

PCR: 03949 Module: IPSEC Level: 3

If a local IP address and remote IP address were not specified in the CREATE IPSEC POLICY command for IPv6 IPSec, the SET IPSEC POLICY configuration was shown unnecessarily in the output of the SHOW CONFIG DYNAMIC=IPSEC command. This issue has been resolved.

PCR: 03952 Module: SWI Level: 3

MAC address are now deleted from the all the internal tables for ports where the learn limit has been exceeded.

PCR: 03954 Module: IPV6 Level: 2

An anycast address could not be assigned when the prefix for the anycast address had previously been assigned on that interface. This issue has been resolved.

PCR: 03958 Module: FIREWALL Level: 2

The ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands no longer accept the GBLREMOTEIP parameter with standard NAT, or enhanced NAT for a private interface.

PCR: 03965 Module: IPSEC Level: 3

IPv6 used the same SA soft expiry timer at both ends of a link, which used memory unnecessarily. This issue has been resolved.

PCR: 03971 Module: SWI Level: 1

A change made in patch 86253-03 caused the Rapier 48 to unexpectedly reboot continuously when powered up. This issue has been resolved.

PCR: 03973 Module: IPG Level: 3

When equal cost multipath routes were used, the IP option field for trace route was not applied correctly. This issue has been resolved.

PCR: 03986 Module: BGP, IPG Level: 2

Route flapping occurred if an interface went down and there was another route to that interface's next hop. This issue has been resolved.

PCR: 31001 Module: DHCP Level: 2

When executing the SET DHCP POLICY, DELETE DHCP POLICY and DESTROY DHCP POLICY commands, memory was not de-allocated correctly. This issue has been resolved.

PCR: 31013 Module: SWI Level: 2

If ports were set to a speed of 100m when creating a switch trunk, the speed could not subsequently be set to 1000m, even if the ports were capable of that speed. This issue has been resolved.

PCR: 31015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 31017 Module: NTP Level: 3

The *RootDispersion* value in NTP packets was negative. RFC 1305 states that only positive values greater than zero are valid. This issue has been resolved.

PCR: 31019 Module: PIM6 Level: 2

The checksum for the PIMv2 *Register* message for IPv6 was not being calculated correctly. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 31028 Module: BGP Level: 2

BGP did not always send *Withdrawn* advertisements when a route went down. This issue has been resolved.

PCR: 31069 Module: IPV6 Level: 2

When adding an IPv6 filter, an error message was displayed stating that the source IP address was not specified, even when the address was specified. This issue has been resolved.

Features in 86253-03

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86253-03.

Base Software Release File	86s-253.rez
Patch Release Date	30-July-2003
Compressed Patch File Name	86253-03.paz
Compressed Patch File Size	191102 bytes

Patch 86253-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 03816 Module: IPG Level: 2

When ports were added or removed as a range with the ENABLE IP IGMP ALLGROUPS and DISABLE IP IGMP ALLGROUPS commands, port values were interpreted as 2 separate ports. This issue has been resolved.

Features in 86253-02

Patch file details are listed in Table 6:

Table 6: Patch file details for Patch 86253-02.

Base Software Release File	86s-253.rez
Patch Release Date	25-July-2003
Compressed Patch File Name	86253-02.paz
Compressed Patch File Size	190900 bytes

Patch 86253-02 includes the following enhancements and resolved issues:

PCR: 03420 Module: IPG, SWI Level: 3

It is now possible to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports. This is enabled with the ENABLE IP IGMP ALLGROUP command, and disabled with the DISABLE IP IGMP ALLGROUP command.

For details, see "*IGMP Snooping All-Group Entry*" on page 46.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03609 Module: OSPF Level: 1

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03657 Module: SWI Level: 3

Executing the DISABLE SWITCH PORT command on a port that was the source of a mirror port did not disable the mirror port. This issue has been resolved.

PCR: 03691 Module: DVMRP Level: 2

A fatal error occurred if the number of DVMRP interfaces being added exceeded the limit. This issue has been resolved.

PCR: 03692 Module: BGP Level: 2

Occasionally a fatal exception may have occurred when sending BGP aggregate routes. This issue has been resolved.

PCR: 03696 Module: IPG Level: 2

IGMP snooping entries were not being deleted from the hardware table. This issue has been resolved. Also, port timers are now updated when the IGMP timeout is changed.

PCR: 03698 Module: DVMRP Level: 3

The output of the SHOW DVMRP FORWARDING command did not display the forwarding ports. This issue has been resolved.

PCR: 03707 Module: STP Level: 2

When adding a port to a VLAN, any STP ports that had been disabled in the default STP were re-enabled. This issue has been resolved.

PCR: 03708 Module: DHCP Level: 2

When the DELETE DHCP RANGE command was executed, DHCP attempted to reclaim the addresses in that range. It also tried to reclaim addresses in that range that were not allocated at that time, resulting in duplicate addresses appearing on the free list for allocation. This has been resolved by allowing DHCP to reclaim only those addresses that are currently in use by one of its clients.

PCR: 03720 Module: STP Level: 2

When changing from RSTP to STP mode, the STPCOMPATIBLE option for the RSTPTYPE parameter incorrectly appeared in the dynamic configuration. Also, when changing from RSTP to STP mode or vice versa, disabled STP ports did not remain in the disabled state. These issues have been resolved.

PCR: 03738 Module: IPG Level: 2

If a port went down, the port was deleted from the appropriate static IGMP associations but was not added back again when it came back up. Similarly, static IGMP associations were automatically deleted but not added back when IP or IGMP was disabled. These issues have been resolved. You can now create IGMP associations before enabling IGMP, and they will become active when IGMP is enabled.

PCR: 03741 Module: FIREWALL Level: 3

The maximum number of firewall sessions had decreased since software release 86s-241. This issue has been resolved.

PCR: 03742 Module: IPV6 Level: 2

Previously, an incorrect source address was used for router advertisements that were sent over an IPv6 tunnel. The source address of the tunnel (specified by the IPADDRESS parameter of the ADD IPV6 TUNNEL command) was used instead of a link local address. This caused an interoperability problem, which has been resolved. Now, if the specified IP address is not a link local address, then a link local address will be created based on the IPv4 tunnel source address and used for router advertisements.

PCR: 03743 Module: IP Level: 3

If a ping was active and the IP configuration was reset, subsequent pings were sent out the wrong interface. This issue has been resolved.

PCR: 03744 Module: PING Level: 3

Executing a ping to the IP address 0.0.0.0 did not return an `invalid destination address` error message. Also, when the TRACE command was executed for local addresses, it timed out after 90 seconds. These issues have been resolved.

PCR: 03764 Module: IPG Level: 3

The IP multicast counter did not increment when IGMP, DVMRP and PIM packets were transmitted and received. This issue has been resolved.

PCR: 03766 Module: FIREWALL Level: 2

The firewall denied streaming data using Windows Media Player 9. This issue has been resolved.

PCR: 03779 Module: DHCP Level: 2

The DHCP client was not honouring a subnet option provided by the DHCP server. This issue has been resolved.

PCR: 03783 Module: IPG Level: 3

The TIMEOUT and SIZE parameters are only valid for the SET IP DNS CACHE command, but no error message was returned if either parameter was specified for the SET IP DNS command. This issue has been resolved.

PCR: 03784 Module: IPV6 Level: 3

Fragmentation of IPv6 packets now complies with RFC 2460's requirement to align packet sizes to 8 octets.

PCR: 03788 Module: DHCP Level: 2

The DHCP server did not send a *DHCPNAK* message when a previously statically assigned IP DHCP entry was again requested by a client. This issue has been resolved.

PCR: 03793 Module: RSVP Level: 3

The ENABLE RSVP INTERFACE command did not succeed if IP was enabled after the RSVP interface had been created. Now, ENABLE RSVP INTERFACE will succeed regardless of when IP is enabled as long as an IP interface exists.

PCR: 03799 Module: DHCP Level: 3

When a new static entry was allocated to a client, an old dynamic entry remained *inuse* for a full lease period. This issue has been resolved. The old entry will now be reclaimed when the client attempts to renew its lease and receives the new static entry.

Enable and Disable ICMP Messages

The *Internet Control Message Protocol* (ICMP) allows routers to send error and control messages to other routers or hosts. It provides the communication between IP software on one system and IP software on another.

This enhancement allows the switch to enable or disable some ICMP messages when directed by the network manager.

The ICMP messages that are able to be enabled or disabled are:

- Network unreachable (RFC792 Type 3 Code 0)
- Host unreachable (RFC792 Type 3 Code 1)
- ICMP redirect messages (RFC792 Type 5 Code 0, 1, 2, 3)

Network Unreachable

This message indicates that the switch does not know how to reach the destination network.

Host Unreachable

This message indicates that the switch does not know how to reach the host.

ICMP Redirect

This message is sent to a local host to tell it that its target is located on the same LAN (no routing is required) or when it detects a host using a non-optimal route (usually because a link has failed or changed its status) on a directly connected router to advise of a better route to a particular destination.

For more information on ICMP, see the IP Chapter in your switch's Software Reference manual.

Commands

This enhancement introduces three new commands:

- DISABLE IP ICMPREPLY
- ENABLE IP ICMPREPLY
- SHOW IP ICMPREPLY

DISABLE IP ICMPREPLY

Syntax

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command disables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are disabled. If NETUNREACH is specified, all network unreachable message replies are disabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are disabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are disabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To disable all configurable ICMP messages, use the command:

```
DISABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ICMPREPLY
DISABLE IP ECHOREPLY
SHOW IP ICMPREPLY

ENABLE IP ICMPREPLY

Syntax

```
ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command enables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are enabled. If NETUNREACH is specified, all network unreachable message replies are enabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are enabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are enabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To enable all configurable ICMP messages, use the command:

```
ENABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ECHOREPLY
DISABLE IP ICMPREPLY
SHOW IP ICMPREPLY

SHOW IP ICMPREPLY

Syntax

```
SHOW IP ICMPREPLY
```

Description This command display the status of configurable ICMP messages (Figure

Figure 2: Example output from the SHOW IP ICMPREPLY command:

```
SHOW IP ICMP REPLY MESSAGES
-------------------------------------------------------------------------------
ICMP REPLY MESSAGES:
  Network Unreachable ............... disabled
  Host Unreachable .................. disabled
  Redirect .......................... enabled
-------------------------------------------------------------------------------
```

Table 7: Parameters in the output of the SHOW IP ICMPREPLY command.

Parameter	Meaning
ICMP Reply Messages	A list of ICMP configurable reply messages and whether they are enabled or disabled.

MLD Snooping

Multicast Listener Discovery (MLD) snooping enables the switch to forward IPv6 multicast traffic intelligently, instead of flooding it out all ports in the VLAN. With MLD snooping, the switch passively listens to MLD joins/reports and leaves/done messages, to identify the switch ports that have received joins and/or leaves from devices attached to them. Multicast traffic will only be forwarded to those ports. MLD snooping will also identify ports that are connected to another router or switch and forward messages out those ports appropriately.

MLD snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will only forward traffic out those ports with routers or IPv6 multicast listeners, therefore it will not act as a simple hub and flood all IPv6 multicast traffic out all ports. MLD snooping is independent of the MLD and Layer 3 configuration, so an IPv6 interface does not have to be attached to the VLAN, and MLD does not have to be enabled or configured.

MLD snooping is enabled by default. To disable it, use the command:

```
DISABLE MLDSNOOPING
```

Note that IPv6 multicast packets will flood the VLAN when MLD snooping is disabled.

To enable MLD snooping, use the command:

```
ENABLE MLDSNOOPING
```

To display debugging information, use the command:

```
ENABLE MLDSNOOPING DEBUG
```

This command displays the ports that are currently receiving MLD packets and the ports that are being added or taken off the switch's multicast group membership registration.

To disable debugging, use the command:

```
DISABLE MLDSNOOPING DEBUG
```

To display information about MLD snooping, use the command:

```
SHOW MLDSNOOPING COUNTER
```

For more information, including limitations on which addresses and packet types can be snooped, see the *IPv6 Multicasting* chapter of the *Software Reference*.

IGMP Snooping All-Group Entry

Because IGMP is an IP-based protocol, multicast group membership for VLAN aware devices is on a per-VLAN basis. If at least one port in the VLAN is a member of a multicast group, multicast packets will be flooded onto all ports in the VLAN by default.

IGMP snooping enables the switch to forward multicast traffic intelligently on the switch. The switch listens to IGMP membership reports, queries and leaves messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

This enhancement allows network managers to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports, by using the ENABLE IP IGMP ALLGROUP command.

For example, consider a video streaming service which has 15 channels. When the switch receives IGMP membership reports destined for the address 239.0.0.2 from an unauthorised user, all 15 channels of multicast data floods to that port, which may affect the service of the network. In order to avoid this, the network manager decides whether or not to allow a particular port to behave as an IGMP all-group port, e.g. port 8. Then, whenever the above IGMP membership report is sent, the switch will not automatically add port 8 as one of the egress ports for any IGMP membership report group, so video streaming will not get forwarded to disabled all-group ports selected by the network manager.

Commands

This enhancement modifies one command:

- SHOW IP IGMP

and has two new commands:

- ENABLE IP IGMP ALLGROUP
- DISABLE IP IGMP ALLGROUP

Modified Command

SHOW IP IGMP

Syntax `SHOW IP IGMP [COUNTER] [INTERFACE=`*`interface`*`]`

Description This command displays information about IGMP, and multicast group membership for each IP interface.

This enhancement includes the line "**Disabled All-groups ports**" on the output of this command, as show in Figure 3 on page 47. Ports that are disabled have a "#" symbol next to the port number.

Figure 3: Example output from the SHOW IP IGMP command.

```
IGMP Protocol
--------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs
Disabled All-groups ports ........ 1,5,7

Interface Name .......... vlan2 (DR)
IGMP Proxy .............. Off
Group List ..............

  Group. 238.0.1.2          Last Adv. 172.50.2.1         Refresh time 34 secs
  Ports 3,11,23

  Group. 224.1.1.2          Last Adv. 172.50.2.1         Refresh time 130 secs
  Ports 2,11,23

  All Groups                Last Adv. 172.50.1.1         Refresh time 45 secs
  Ports 1#,11,23


Interface Name .......... vlan4             (DR)
IGMP Proxy .............. Off
Group List ..............
  No group memberships.

--------------------------------------------------------------------------------
```

Table 8: New parameter in the output of the SHOW IP IGMP command.

Parameter	Meaning
Disabled All-groups ports	A list of ports that are prevented from behaving as IGMP all-group ports.

Examples To show information about IGMP, use the command:

```
SHOW IP IGMP
```

See Also ENABLE IP IGMP ALLGROUP
DISABLE IP IGMP ALLGROUP

New Commands

This enhancement request introduces two new commands from enabling/ disabling all-group entries on switch ports.

ENABLE IP IGMP ALLGROUP

Syntax `ENABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 ad end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command enables the specified port(s) to behave as a multicast all-group ports.

The ALLGROUP parameter specifies the list of ports able to behave as all-group entry ports. If ALL is specified, all ports are able to behave as all-group entry ports. The default is ALL.

Examples To enable ports 1, 5 and 7 to behave as all-group entry ports, use the command:

```
ENABLE IP IGMP ALLGROUP=1,5,7
```

See Also DISABLE IP IGMP ALLGROUP
SHOW IP IGMP

DISABLE IP IGMP ALLGROUP

Syntax `DISABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command disables the specified port(s) from acting as a multicast all-group entry ports. Ports that are disabled have a "#" symbol next to the port number in the output of the SHOW IP IGMP command.

Examples To prevent ports 1, 5 and 7 from behaving as all-group entry ports, use the command:

```
DISABLE IP IGMP ALLGROUP=1,5,7
```

See Also ENABLE IP IGMP ALLGROUP
SHOW IP IGMP

Ping Polling of Device Reachability

This enhancement enables the router or switch to regularly check whether or not it can reach a device. It also enables a trigger to activate on the router or switch when the device becomes unreachable. While the device is unreachable, the router or switch continues to monitor the device's reachability, and another trigger can be set to activate when the device becomes available again. For example, the first trigger's script could open and configure an alternative link if the device at the other end of a preferred link became unavailable. The second trigger's script would automatically return traffic to the preferred link as soon as it was available again.

To determine the device's reachability, the router or switch will regularly send ICMP Echo Request packets ("pings") to the device. As long as the router or switch receives ping responses from the device, it considers the device to be reachable. After the router or switch has not received a reply to a set number of ICMP Echo Requests, it considers the device to be unreachable. It continues to try to ping the device, at an increased rate. After it receives a set number of responses, it considers the device to be reachable again.

Configuring the router or switch to determine a device's reachability and respond to changes in reachability involves the following steps:

- Create a polling instance, to periodically ping the device
- Create scripts to run when the device becomes unreachable and when it becomes reachable again
- Configure triggers to run these scripts.

To create a polling instance, use the command:

```
ADD PING POLL=poll-id IPADDRESS={ipadd|ipv6add[%interface]}
    [CRITICALINTERVAL=1..65535]
    [DESCRIPTION=poll-description] [FAILCOUNT=1..100]
    [LENGTH=4..1500] [NORMALINTERVAL=1..65535]
    [SAMPLESIZE=1..100] [SIPADDRESS={ipadd|ipv6add}]
    [TIMEOUT=1..30] [UPCOUNT=1..100]
```

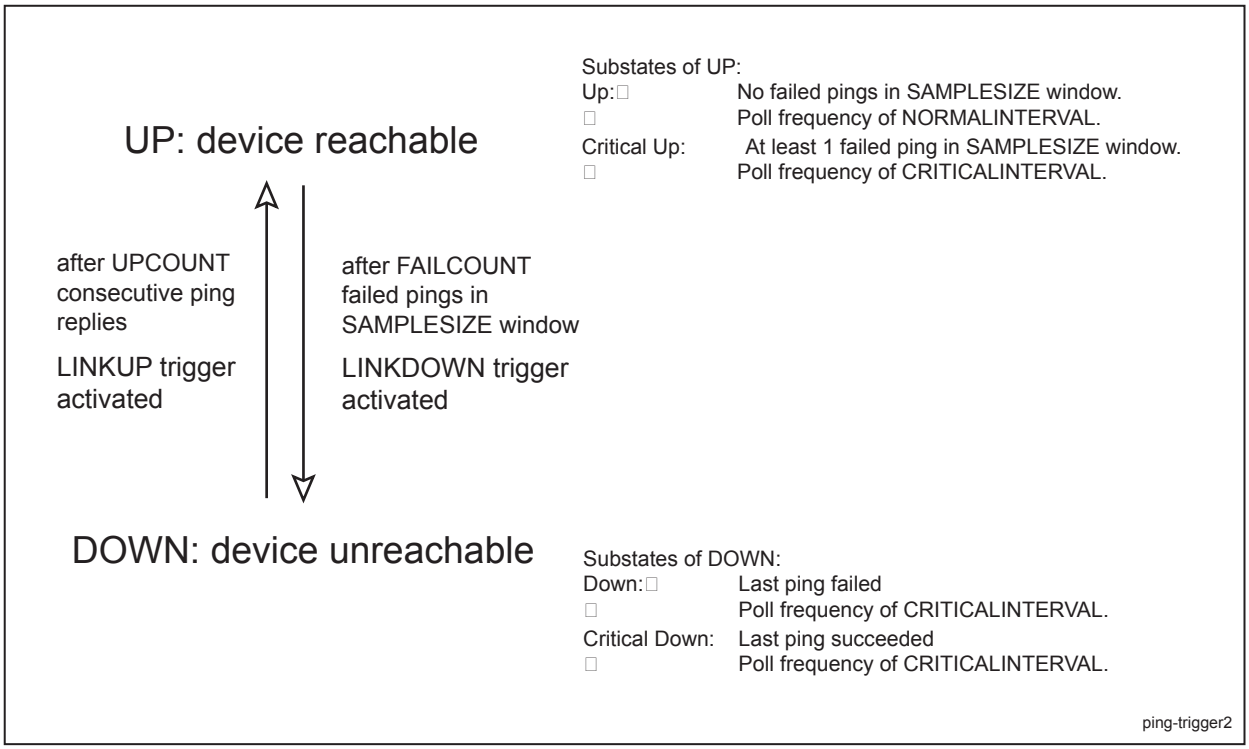
- where *poll-id* is a number from 1 to 100, and identifies the polling instance in the trigger commands and in other PING POLL commands. The router or switch can poll up to 100 IP addresses at once.

The NORMALINTERVAL parameter specifies the time period between pings when the device is reachable. By default, this is set to 30 seconds. The CRITICALINTERVAL parameter specifies the time period between pings when the router or switch has not received a reply to at least one ping and when the device is unreachable. The default is 1 second. The CRITICALINTERVAL enables the router or switch to quickly observe changes in the state of the device, and should be set to a much lower value than the NORMALINTERVAL.

The number of pings that the router or switch will examine to consider a change in state is controlled by three parameters: FAILCOUNT, SAMPLESIZE, and UPCOUNT. The FAILCOUNT is the number of pings that must be unanswered for the router or switch to consider the device unreachable. The default is 5. The SAMPLESIZE is the total number of pings within which the FAILCOUNT number of pings must be unanswered. If SAMPLESIZE and FAILCOUNT are the same, the unanswered pings must be consecutive. If SAMPLESIZE is greater than FAILCOUNT, a device that does not always reply to pings may be declared unreachable. By default, SAMPLESIZE is equal to

FAILCOUNT. The UPCOUNT is the number of consecutive pings that must be answered for the router or switch to consider the device reachable again. The default is 30. The interaction between these parameters is shown in Figure 4.

Figure 4: The interaction between states and parameters for ping polling.



After you have configured the ping polling instance, specify a script or scripts to run when the device becomes unreachable, using the command:

```
CREATE TRIGGER=trigger-id MODULE=PING EVENT=DEVICEDOWN
   POLL=poll-id SCRIPT=filename... [other-options...]
```

Then specify a script or scripts to run when the device becomes reachable again, using the command:

```
CREATE TRIGGER=trigger-id MODULE=PING EVENT=DEVICEUP
   POLL=poll-id SCRIPT=filename... [other-options...]
```

where *filename* is the name of the script file, and will have a `.scp` extension.

Finally, enable the polling instance, using the command:

```
ENABLE PING POLL=poll-id
```

Ping polling is only available for IP and IPv6 (ICMP and ICMP6 Echo Request and Reply packets), not for IPX, AppleTalk or OSI.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.